No. 17-2

IN THE

Supreme Court of the United States

UNITED STATES OF AMERICA,

Petitioner,

v.

MICROSOFT CORPORATION,

Respondent.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

BRIEF FOR DIGITALEUROPE, BITKOM, TECH IN FRANCE, SYNTEC NUMÉRIQUE, AND OTHER EUROPEAN NATIONAL TRADE ORGANIZATIONS AS *AMICI CURIAE* SUPPORTING RESPONDENT

ILANA H. EISENSTEIN
Counsel of Record
ETHAN H. TOWNSEND
JOHN M. LEITNER
LINDSAY R. BARNES III
DLA PIPER LLP (US)
One Liberty Place
Philadelphia, PA 19109
(215) 656-3300
ilana.eisenstein@dlapiper.com

Counsel for Amici Curiae

278321

COUNSEL PRESS
(800) 274-3321 • (800) 359-6859

TABLE OF CONTENTS

Page

TABLE OF CONTENTS i

TABLE OF CITED AUTHORITIES iii

INTEREST OF *AMICI CURIAE* 1

SUMMARY OF ARGUMENT 3

ARGUMENT 6

I. Remote Data Storage Is Essential To Modern Business And Social Practices 6

II. Data Privacy Should Be Addressed Through Multilateral Agreement, Not By Unilateral Fiat 9

III. The Government's Position Would Create An Unnecessary And Serious Conflict With E.U. Data Privacy Rules Including The GDPR 11

IV. The Government's Unilateral Approach To Data Privacy Will Harm The Economy, Disrupt Business Relations, And Encourage The Enactment Of Unfavorable Foreign Policies 16

A. Unilateral Data Policies Will Have A Chilling Effect On The Free Flow Of Information Over The Internet 17

Table of Contents

Page

B. The Government's Position Would Embolden Other Countries To Exercise Reciprocal Authority To Access Data Stored In The United States 20

V. The United States Has Multilateral Options And Other Less Disruptive Alternatives To Obtain Data From Foreign Servers 21

CONCLUSION 24

APPENDIX 1a

TABLE OF CITED AUTHORITIES

Page

CASES

EEOC v. *Arabian American Oil Co.*, 499 U. S. 244 (1991) 10

Kiobel v. *Royal Dutch Petroleum*, 569 U.S. 108 (2013) 10

STATUTES

Cybersecurity Law of the People's Republic of China (promulgated by the Standing Comm. Nat'l People's Cong. Nov. 7, 2016, effective Jun. 1, 2017) 18

German Federal Data Protection Act, June 30, 2017, 2017.7.5 BGBI 14, 15

Judicial Redress Act of 2015, Pub. L. No. 114-126, 130 Stat. 282 22

Stored Communications Act, Pub. L. No. 99-508, Tit. II, 100 Stat. 1860 (18 U.S.C. § 2701 *et seq.*) ..... *passim*

OTHER AUTHORITIES

E.U.'s General Data Protection Regulation, Art. 3(1) 12

Cited Authorities

Page

E.U.'s General Data Protection Regulation, Art. 4(1) 13

E.U.'s General Data Protection Regulation, Article 48 ..... 4, 13

E.U.'s General Data Protection Regulation, Article 49 ..... 13, 14

E.U.'s General Data Protection Regulation, Art. 83(5)(c) 15

European Commission, Building a European Data Economy, Digital Single Market Strategy (Jan. 10 2017) 8

European Commission, *Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy* (October 2017) 6

European Commission, Digital Single Market: Bringing Down Barriers To Unlock Online Opportunities, EC.EUROPA.EU 18

European Convention on Human Rights, Article 8 11

Government of India Ministry of Science & Technology, India's National Data Sharing and Accessibility Policy (2012) 18

Cited Authorities

Page

Konstantinos Giannakouris, Maria Smihily, Eurostat Statistics Explained, Cloud computing - statistics on the use by enterprises (Feb. 28, 2017) 8

Louis Columbus, Forbes, Cloud Computing Market Projected To Reach $411B By 2020 (Oct. 18, 2017) 8

Nigel Cory, Information Technology and Innovation Foundation, Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? (May 1, 2017) 19

Treaty between the Federal Republic of Germany and the United States of America on Mutual Legal Assistance in Criminal Matters of 14 October 2003, as amended, Art. 11 14

Treaty on the Functioning of the European Union, Art. 16(1), 2012 O.J. C 326/55.....11

U.S.-Ireland Mutual Legal Assistance Treaty, Art 1 § 1; § 2(b), (f).....21

U.S. Policymakers and Industry Leaders, 2 *Lawfare Research Paper Series* (July 21, 2014).....19

U.S. Attorneys' Manual, Criminal Resource Manual § 276, "Letters Rogatory" 22

INTEREST OF AMICI CURIAE[1]

Principal Parties of Interest

DIGITALEUROPE is the leading trade organization that represents the digital technology industry in Europe. Its 62 corporate members and 37 national trade association members include some of the world's largest information technology, telecommunications and consumer electronics companies and national trade associations from every part of Europe.[2] DIGITALEUROPE is actively engaged in shaping data protection law and policy in Europe by publishing policy papers, offering strategic advice, and participating as amicus curiae in European courts. DIGITALEUROPE has a vested interest in fostering a business, policy, and regulatory environment that nurtures and supports digital technology industries.

BITKOM is an association of companies in the digital technology industry in Germany. BITKOM represents more than 2,500 companies in the digital economy across sectors, including software and information technology, telecommunications and internet services, hardware and consumer electronics manufacturers, and digital media.

---

1. All parties have consented to the filing of this brief by blanket consent or letter. No counsel for a party has authored this brief in whole or in part. Respondent, Microsoft Corporation, is one of DIGITALEUROPE's 62 corporate members. Otherwise, no person other than amici curiae, its members, and its counsel have made monetary contributions to the preparation or submission of this brief.

2. DIGITALEUROPE's members are listed in Appendix A to this brief.

BITKOM has taken a leading role in helping to craft European data protection law as an advocate for innovative economic policies, the modernization of the European educational system, and forward-looking network policies. On behalf of its members, BITKOM works to cultivate law and policy that encourages ingenuity and progress in the digital field.

TECH IN France is a coalition of digital technology companies in France. The 400 members of TECH IN France include large companies, small-to-medium enterprises, and start-ups. In lobbying on behalf of the digital technology sector and devising and promoting best practices, TECH IN France has led the industry-wide effort to promote investment in the French digital economy. As such, TECH IN France has been a key player in the development of European data protection law and continues to champion law and policy aimed at unleashing the potential of the digital technology industry for France, Europe, and the world at large.

Syntec Numérique is a French national trade association representing digital services companies, software publishers, and technology consulting firms. Syntec Numérique brings together 2,000 member companies who, combined, generate 80% of the sector revenue in France (more than €50 billion in revenue and 447,000 employees in the sector). Syntec Numérique contributes to the promotion and growth of the Internet and technology sector through the development of the digital economy and its uses, support and the development of new markets, support for the digital economy, employment, training, services to members and the defense of the interests of the profession. Syntec Numérique is part

of the Syntec Federation which brings together in its constituent unions more than 3,000 French groups and companies specializing in the fields of Engineering, Digital, Studies and Consulting, Professional Training, and Events. Since 2013, Syntec Numérique has been a member of DIGITALEUROPE.

Supporting Parties in Interest

The Federation of Hellenic Information Technology & Communications Enterprises (SEPE) represents 250 members in Greece.

The Association of Electronics, Information and Communications Technologies, Telecommunications and Digital Content Companies (AMETIC) represents 250 members in Spain.

SUMMARY OF ARGUMENT

This Court should affirm the Second Circuit's decision, which correctly concluded that the Stored Communications Act (SCA)[3] has clear territorial limits that confine its authority to the United States. By contrast, the government's expansive interpretation of the SCA would gravely intrude on the regulatory authority of the European Union (E.U.) and its member nations, stoke unnecessary conflict between United States and E.U. regulation, and force corporations attempting to comply with both regimes into an untenable position.

---

3. Pub. L. No. 99-508, Tit. II, 100 Stat. 1860 (18 U.S.C. 2701 *et seq.*).

In the modern digital economy, technology companies routinely store data remotely through cloud computing, rather than rely on local hard drives or attached servers. Data is stored remotely for both business and technical reasons, including to improve service delivery to consumers, increase network efficiency, promote resilience, enhance security, and decrease costs. There are substantial business, economic, and social benefits to fostering the free flow of information across national borders.

National sovereignty does not disappear merely because private companies choose, for market-driven reasons, to use cloud computing and remote data storage. Rather, the storage, collection, and transfer of personal data is a sensitive, multilateral issue with broad economic and foreign policy implications. The execution of an SCA warrant would allow United States law enforcement to reach into Europe (or another foreign jurisdiction) to access customer data in a manner that intrudes on the E.U.'s sovereign interests and its prerogative to regulate the processing and transfer of data within its borders.

Of particular concern to amici is a looming clash between the government's expansive view of the SCA's warrant authority and the E.U.'s General Data Protection Regulation (GDPR), which goes into effect on May 25, 2018. The GDPR is a robust regulatory regime that addresses the operation of modern data systems and asserts control over the processing and control of data within the E.U.'s territorial authority. The GDPR's Article 48 strictly limits the circumstances under which a company can process or transfer an E.U. subject's data in response to a foreign (non-E.U.) law enforcement

demand. If the government's view of the SCA prevails, companies may have to choose between defiance of a U.S. warrant or the risk of substantial administrative, monetary, or even criminal penalties if the data transfer runs afoul of the E.U.'s stringent data protection rules. That potential conflict will acutely affect almost every industry stakeholder in the technology community.

The government's unilateral approach to international data warrants would harm the technology industry, including amici's members, in other ways. Companies may increasingly block cross-border access to data to avoid liability and to satisfy market demand for privacy protection. The partition of the Internet along national borders would adversely affect hundreds of millions of customers who rely on seamless access to data and the other benefits of cloud computing. It also may erode the trust of consumers who rely on the application of E.U., not United States, data privacy rules. Those customers may hesitate to entrust their data to technology companies that are within the reach of the U.S. criminal process.

The foreign policy implications of the government's position are also troubling. The government's position may push other countries to retreat from the digital economy and accelerate the trend toward data localization laws that restrict the flow of information across borders. That development would harm U.S. economic and diplomatic interests and inhibit the full potential of the Internet. In addition, if the government's position were the rule, other countries would be able to claim the reciprocal authority to seize data stored in the United States and transfer it abroad without regard to U.S. privacy regulations.

This case is about respecting other nations' laws and processes. This Court should not to adopt the government's argument that the SCA permits unilateral demands for data controlled and housed abroad. Multilateral solutions, including existing mutual legal assistance treaties (MLATs), already serve law enforcement interests in obtaining foreign evidence while respecting sovereign and territorial limits. To the extent that the government requires new tools to address innovations in data technology, those solutions should be developed through diplomatic, not unilateral, action. Amici strongly urge this Court to adopt an interpretation of the SCA that is consistent with a multi-lateral approach to data collection and transfer.

ARGUMENT

I. Remote Data Storage Is Essential To Modern Business And Social Practices

The modern global economy is driven not just by the flow of goods, but by the flow and exchange of data.[4] Reliance on data flow across borders has become critical to nearly every industry, ranging from companies and products that facilitate the creation and communication of digital content (*e.g.*, Facebook or Twitter) to traditional

4. In fact, in recent years, the economic value of cross-border movement of data has been estimated to exceed the value of the movement of goods. European Commission, ***Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy***, (Oct. 1, 2017), https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy (last visited Jan. 15, 2018).

industries that maintain competitiveness by taking advantage of new methods of data storage and processing.[5] If SCA warrants were to apply to data stored outside of the United States, businesses may retreat from global technological advancement to avoid the government's extraterritorial reach. The economic and social costs of that retreat could be substantial.

Just as the rise of transportation networks and international trade once transformed the identity of manufacturers from local operations to national and international firms, the rise of the global digital economy has now altered the basic structure of how and where businesses store and utilize information to deliver products and services to consumers. An open Internet that facilitates the free flow of data across borders is a critical underpinning of modern economic markets in the 21st Century.

Diverse and innovative data storage models facilitate the flow and management of data to address business needs and market demands. "Cloud computing" is a rapidly growing model that provides access to data and application services remotely via the Internet. Cloud computing accommodates the surging demand for fast, inexpensive, and secure technology, computing, and digitization services. In the process, cloud computing has become a sizable and highly productive industry in its own right. The successful implementation of cloud computing has become a foundational element of secure and high-speed access to data.

---

5. McKinsey Global Institute, *Digital Globalization: the New Era of Global Flows* (2016).

Cloud computing has grown steadily year after year. The 2017 U.S. cloud computing market is estimated at approximately $260 billion; and it is expected to expand to more than $400 billion per year by 2020. The European Commission has projected that the E.U. data economy will be worth €739 billion (*i.e.*, 4% of the E.U.'s overall GDP) by 2020.[6] This striking growth model signals an explosion in demand for cloud computing services.

The increased use of remote data storage in diverse and multinational locations is a consequence of technical improvements and business incentives. Its rapid growth is not driven, therefore, by any corporate impetus to evade law enforcement. Instead, cloud computing may occur across borders because, quite simply, the Internet is a transnational enterprise. Data is stored where that storage is secure and cost-effective and where it can be retrieved in a manner that meets business and consumer needs.[7]

---

6. European Commission, Building a European Data Economy, Digital Single Market Strategy (Jan. 10, 2017), https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy (last visited Jan. 15, 2018).

7. See Konstantinos Giannakouris, Maria Smihily, ***Cloud computing - statistics on the use by enterprises***, Eurostat Statistics Explained, (Feb. 28, 2017, 9:47 PM), http://ec.europa.eu/eurostat/statisticsexplained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises#Use_of_cloud_computing:_highligh (last visited Jan. 15, 2018); Louis Columbus, ***Cloud Computing Market Projected to Reach $411B by 2020***, Forbes (Oct. 18, 2017, 6:12 PM), https://www.forbes.com/sites/louiscolumbus/2017/10/18/cloud-computing-market-projected-to-reach-411b-by-2020/#13acef0878f2 (last visited Jan. 15, 2018).

II. Data Privacy Should Be Addressed Through Multilateral Agreement, Not By Unilateral Fiat

National sovereignty does not disappear merely because private companies choose to store data abroad for market reasons. The Internet's global reach means that the regulation of personal data privacy has become a highly sensitive, multilateral issue. The preferred approaches, advocated by amici, are government-to-government solutions and agreements that facilitate cross-border access to electronic evidence in a way that respects the sovereignty of the countries involved, including a nation's power to advance what it may regard as important fundamental rights to personal privacy.

The government brushes those considerations aside by denying that compliance with an SCA warrant for data stored abroad "would create an extraterritorial violation of privacy." Gov't Br. 29. The government reasons that access to and production of data stored abroad requires only "domestic disclosure of information," and that the process of "collect[ing] data" stored in Europe is a mere "preparatory step" to its disclosure. *Id.* at 26.

The government's premise is incorrect both as a technical matter and as a legal matter. Access to data stored abroad requires an actual physical extraction of data from that foreign location. The government's claim that Microsoft could access data located on a server in Ireland from a computer in Redmond, Washington, considers only the location where a search query is made, and not where the search is run or where the source data is identified and transferred. In this case, at the moment that a person sitting at a computer in Redmond initiates

a search for that data, it is only located, in digital form, on a server within the territory of Ireland. The capacity of a person to copy and transfer (or extract and transfer) that data to another jurisdiction does not eliminate the pre-existing territorial nexus between that data and the location where it was controlled and processed.

More fundamentally, the government unduly minimizes the staggeringly broad authority that it asserts to reach into Europe (or another foreign country) to access customer data. See Gov't Br. 32-41. Extending U.S. law enforcement authority to allow it to access foreign-controlled data intrudes on sovereign interests, implicates sensitive foreign policy questions, and creates a serious potential for conflicts of law—each of the factors cautioning against extraterritoriality that this Court identified in *Kiobel* v. *Royal Dutch Petroleum Co.*, 569 U.S. 108, 133 (2013), and *Equal Employment Opportunity Commission* v. *Arabian American Oil Co.*, 499 U.S. 244, 248 (1991).

Those concerns are underscored by the fact that the E.U. and its member nations treat the storage and transfer of data located within its borders as subject to the law and regulations of the E.U. and its members. See E.U. Commission Amicus Br. (E.U. Br.) 8. The E.U. has devised detailed and comprehensive regulations governing the processing, collection, control, storage, and transfer of data within its borders. It did so only through painstaking legal and regulatory processes rooted in fundamental principles of personal rights to privacy under E.U. law.[8]

8. The privacy limits on the collection and processing (including transfer) of personal data are established by the

This Court should not conclude that Congress would lightly disregard the carefully reticulated privacy regime established by the E.U.

III. The Government's Position Would Create An Unnecessary And Serious Conflict With E.U. Data Privacy Rules Including The GDPR

Although the E.U. and its members have long regulated the collection, storage, and transfer of personal data, amici are particularly concerned that the government's interpretation of the SCA will pose an imminent and serious conflict with the GDPR, which goes into effect on May 25, 2018. The GDPR places strict limits on data transfers from E.U. nations to other countries in response to foreign law enforcement demands. If the government's view of the SCA prevails, companies will be forced to choose between compliance with an SCA warrant and the risk of substantial administrative, monetary, or even criminal penalties if the data transfer ran afoul of the E.U.'s stringent data protection rules. That potential

---

foundational documents of E.U. law. See Council of Europe, European Convention on Human Rights, as amended by Protocol Nos. 11 and 14, supplemented by Protocols Nos. 1, 4, 6, 7, 12, and 13, Art. 8 available at http://www.echr.coe.int/Documents/Convention_ENG.pdf (last visited Jan. 15, 2018) ("Everyone has the right to respect for his private and family life, his home and his correspondence."); Charter of Fundamental Rights of the European Union, Art. 8, 2000 O.J. C 364/10. ("Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned."); Treaty on the Functioning of the European Union (TUE), Art. 16(1), 2012 O.J. C 326/55 ("Everyone has the right to the protection of personal data concerning them.").

conflict will dramatically impact almost every industry stakeholder in the technology community, including amici and its members.

The E.U. passed the GDPR in 2016, after four years of research, analysis, and negotiation among its member nations. The full GDPR comprises 99 articles that comprehensively regulate, standardize, centralize, and strengthen protection of personal data privacy, including data collection, processing, and transfer of data to "third countries" (nations not members of the E.U.).[9] The GDPR affirms the E.U.'s authority over data residing on European servers collected from E.U. residents. See E.U. Br. 8. And it will, among other things, require companies to adhere to the GDPR's regulation of data processing, which includes collection, storage, and *transfer* of personal data from the E.U. to foreign locations. GDPR, Art. 3(1) (emphasis added); see E.U. Br. 8 ("The 'processing' of personal data * * * in the European Union is regulated by E.U. privacy law under the GDPR.").

---

9. As expressed in Recital 101 of the GDPR, "[W]hen personal data are transferred from the [E.U.] to controllers, processors or other recipients in third countries or to international organisations [sic], the level of protection of natural persons ensured in the [E.U.] by this Regulation should not be undermined * * * transfers to third countries and international organisations [sic] may only be carried out in full compliance with this Regulation." Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR), Recital 101, 2016 O.J. L 119/19.

Article 48 of the GDPR regulates access by foreign (non-E.U.) law enforcement to personal data that is controlled and processed within the E.U. GDPR, Art. 48. Article 48 provides that a technology company that processes or controls data[10] cannot comply with a foreign warrant "to *transfer* or *disclose* personal data" if the warrant was not "based on an international agreement such as [an MLAT]" between the United States and the E.U. or a Member State. GDPR, Art. 48 (emphasis added). The SCA warrant in this case was a unilateral demand for information; it was not the product of an MLAT or other international agreement.[11] That SCA warrant would not meet Article 48's requirements for the transfer of data from Europe to U.S. law enforcement.

Other provisions of the GDPR may allow data transfers to foreign law enforcement without an MLAT or similar international agreement. For example, Article 49 permits data transfers for "important reasons of public interest" identified in E.U. or its members' laws. Art. 49(1)(d), GDPR. That provision also allows data transfers "necessary for the purposes of compelling legitimate interests pursued by the controller which are not

---

10. The GDPR uses the term "controller" or "processor." A "controller" is an entity responsible for keeping and maintaining personal data on computer or server. See GDPR Art. 4(1), 2016 L 119/33. (defining "controller" as the entity that "determines the purposes and means of the processing of personal data") A "processor" "processes personal data on behalf of the controller." *Ibid.*

11. In other instances, an SCA warrant may be issued in furtherance of a mutual legal assistance treaty. See 18 U.S.C. 2711(3)(A)(iii) ("court of competent jurisdiction" may issue an SCA warrant "acting on a request for foreign assistance").

overridden by the interests or rights and freedoms of the data subject." Art. 49(1)(g), GDPR. Those exceptions could include law enforcement priorities such as combatting money laundering, international drug trafficking, antitrust violations, and other serious crimes.[12] Nonetheless, the precise contours of those exceptions are not well-defined and will be determined by each member nation's own data protection authorities, which are responsible for interpretation and enforcement of the regulations.

E.U. member nations also have enacted similar data privacy regulations. For instance, German law proscribes the transfer of personal data from Germany to other countries other than under the conditions set forth in Germany's operative data privacy law. German Federal Data Protection Act, § 78.[13] German law does not recognize a foreign search warrant unless it is enforced through an MLAT or other statutory instrument issued by a German court. The conditions for search and seizure are addressed in detail in the MLAT between Germany and the United States.[14]

In any given case, it would be difficult for a company to be certain whether the GDPR authorizes the transfer of data from the E.U. to the United States pursuant to an SCA warrant. That company would likewise have to

---

12. See GDPR, Art. 49, 2016 O.J. L 116/64-65; see also E.U. Br. 15.

13. German Federal Data Protection Act, June 30, 2017, 2017.7.5 BGBI, pp. 2097-2132.

14. See Treaty between the Federal Republic of Germany and the United States of America on Mutual Legal Assistance in Criminal Matters of 14 October 2003, as amended, Art. 11.

determine whether the transfer satisfied the requirements applicable under the law of E.U. member nations.[15]

The stakes are extremely high. The GDPR imposes severe penalties for violation of its requirements. The penalties for noncompliance could be *4% of a company's global revenue* or €20 million, ("*whichever is higher*"). GDPR, Art. 83(5)(c) (emphasis added). The government's view of the SCA threatens to place corporations operating in both the United States and the E.U. in an untenable position: forced on the one hand to defy a U.S. warrant seeking data stored abroad, or, on the other, to risk substantial penalties under the GDPR if it complies with a unilateral U.S. warrant without meeting the GDPR's strict requirements for data transfers to foreign law enforcement.

Companies and their employees also face potential criminal liability in individual European countries for violations of their data transfer restrictions. For example, the German Parliament (Bundestag) passed a new Federal Data Protection Act (Bundesdatenschutzgesetz) codifying the GDPR and imposing a prison sentence for certain GDPR violations up to three years.[16] It would only increase the stakes if other countries follow

---

15. The government's proposal that the SCA warrant be treated like a subpoena does not alleviate those concerns. Gov't Br. 34-39. The GDPR does not distinguish between a foreign warrant and a law enforcement subpoena. In either case, the GDPR's data transfer restrictions have equal force and proscribe extraction of European data pursuant to foreign, unilateral court orders.

16. German Federal Data Protection Act, June 30, 2017, 2017.7.5 BGBI, § 42(1).

Germany's lead and add their own criminal penalties to potentially debilitating administrative fines.

If the SCA applies to data stored in the E.U., as the government asserts, the impending clash between the SCA and the GDPR would acutely affect almost every industry stakeholder in the technology community, and would put the technology industry in an untenable bind. This Court should not conclude that the SCA was meant to create such an intractable conflict.

IV. The Government's Unilateral Approach To Data Privacy Will Harm The Economy, Disrupt Business Relations, And Encourage The Enactment Of Unfavorable Foreign Policies

The government's unilateral approach to seeking, gathering, and transferring data cross-border would harm the technology industry, including amici's members, in other ways. The fear of liability and the demand for increased privacy protection may pressure companies to isolate their data geographically by blocking data access across borders, leading the Internet and data services to be fragmented, less efficient, and more costly. Customers in the E.U., moreover, rely on the application of European, not United States, data privacy rules. Access to E.U. customer data by the United States would cause customers to lose faith in U.S. technology services. And the government's proposed extension of U.S. access to foreign data may prompt foreign governments to require data localization, to prohibit information sharing, and to seek reciprocal access to data in the United States. Those business and foreign policy shifts would adversely affect millions of customers who rely on seamless access to data and utilization of cloud computing.

A. *Unilateral Data Policies Will Have A Chilling Effect On The Free Flow Of Information Over The Internet*

The conflicts posed by extraterritorial and unilateral data policies will discourage the free flow of digital information, hamstring the growth of cloud computing, and limit technology's potential to increase efficiency, lower costs, and enhance security and privacy.

To tap into the full economic potential of the Internet, information must be able to flow freely across national borders. But, to avoid being caught by conflicting national data protection regulations, corporations will be increasingly pressured to segregate data according to national lines, for example, by blocking access to foreign data from U.S.-based employees. Such a move would undermine the core efficiency of the digital age—the free flow of data and information across boundaries.

A unilateral approach to data access also could threaten consumer trust. Much like the privacy guaranteed by Swiss bank accounts, computing company customers that have data stored within the E.U. rely upon the security and privacy that is the cornerstone of the GDPR. Those customers will necessarily be dismayed if the robust structure of the privacy protections in the E.U. can so easily be run over by the United States. That concern is not hypothetical. Several of amici's member companies, including Verizon, Cisco, and Hewlett-Packard, filed an amicus brief in the court of appeals that estimated that U.S. companies lost up to $180 billion in revenues due to foreign consumers' mistrust of U.S. authorities, and their fear that the United States would have access to

their personal data stored abroad. Amicus Br. of Verizon Commc'ns Inc., et al. at 10-15 & n.7, No. 14-2985 (2d Cir. Dec. 15, 2014).

Out of a desire to protect their citizens' data from extraterritorial access by foreign governments, nations also may retreat from the digital economy by implementing "data localization laws" that restrict the storage and transfer of information to a nation's territorial limits. A global trend toward data localization is already underway among some of the world's economic powers. For example, in June 2017, China enacted a new "National Security Law" that requires "critical information infrastructure operators" to store certain personal and business information within China.[17] India similarly has both proposed and implemented policies that restrict the flow of data across its borders, creating significant issues for small business innovators seeking to expand into the Indian market.[18]

The E.U. has generally pushed against data localization, including by sponsoring an initiative to create a "Digital Single Market" to promote "the free movement of goods, persons, services, capital and data."[19] But the issue of

17. Cybersecurity Law of the People's Republic of China (promulgated by the Standing Comm. Nat'l People's Cong. Nov. 7, 2016, effective Jun. 1, 2017).

18. Government of India Ministry of Science & Technology, India's National Data Sharing and Accessibility Policy, (2012), available at http://ogpl.gov.in/NDSAP/NDSAP-30Jan2012.pdf.

19. European Commission, Digital Single Market: Bringing Down Barriers To Unlock Online Opportunities, EC.EUROPA.EU, https://ec.europa.eu/commission/priorities/digital-single-market_en (last visited Jan. 10, 2018).

data localization is controversial among E.U. nations; France and Germany, for example, continue to pressure the E.U. for greater latitude to require local storage and retention of data.[20]

Any acceleration of the corporate and national trend toward data localization policies would cause economic, social, and technological harms. Localization restricts the free flow of data, limits competition, increases costs, inhibits free expression, and stymies innovation. As one commentator noted, data localization will "profoundly fragment[] the Internet, turn[] back the clock on the integration of global communication and ecommerce, and put[] into jeopardy the myriad of societal benefits that Internet integration has engendered."[21]

The government's brief argues that innovative and diverse systems for data storage justify its extraterritorial interpretation of the SCA. Gov't Br. 43. It notes, for example, that there are companies that "store[] the emails of U.S. users all over the world," such that the precise location of data may not be known at any given

---

20. Nigel Cory, *Information Technology and Innovation Foundation, Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, Information Technology & Innovation Foundation (May 1, 2017), available at https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.

21. Jonah Force Hill, *The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders*, 2 Lawfare Research Paper Series 4 (July 21, 2014), available at https://lawfare.s3-us-west-2.amazonaws.com/staging/Lawfare-Research-Paper-Series-Vol2No3.pdf (last visited Jan. 15, 2018).

time. See *id.* at 43-44. To be sure, such innovative data storage models blur territorial and sovereign lines. But the freedom to utilize such international technological capabilities may become a luxury of the past if countries like the United States seek to exercise unilateral control of data abroad, rather than address those complexities through multi-lateral agreement.

B. *The Government's Position Would Embolden Other Countries To Exercise Reciprocal Authority To Access Data Stored In The United States*

If this Court interprets the SCA to allow U.S. law enforcement agencies to reach unilaterally into foreign servers located in the E.U. to extract and transfer user data, the United States may soon see an in-kind response from other countries. Under the principle of reciprocity, nations may adopt laws that would force service providers to produce data stored in the United States. The court of appeals aptly observed that the risks of foreign response are "most easily appreciated if we consider the likely American reaction if France or Ireland or Saudi Arabia or Russia proclaimed its right to regulate conduct by Americans within our borders."[22] That reciprocity principle illustrates the dangers of a broad-reaching, extraterritorial interpretation of the SCA—it gives license to foreign governments to reach into U.S. servers for the private data of U.S. citizens. It also highlights the potential for foreign conflict, the intrusion on sovereignty, and risks to data privacy of the government's unilateral approach.

---

22. Pet. App. 55a-56a.

V. The United States Has Multilateral Options And Other Less Disruptive Alternatives To Obtain Data From Foreign Servers

The government does not need to resort to SCA warrants to obtain data stored abroad. Rather, existing law provides mechanisms for obtaining data without disregarding foreign data regulations. To the extent that existing mechanisms are insufficient, this Court should not strain the SCA to extend it broadly to data that is subject to foreign regulation. Legislative and diplomatic solutions that balance domestic law enforcement priorities with the sensitive foreign policy questions and business needs presented by this issue are the appropriate course.

For example, the government could have pursued an MLAT for the data in this case. Of the 28 E.U. members, the United States has entered into MLATs of one kind or another with 20 of them—including Ireland, where the servers in this case were located.[23] In fact, the Irish government submitted a brief that recognized its MLAT with the United States, argued that the MLAT would be the appropriate channel for the United States to obtain the requested data, and agreed to cooperate with the U.S. government. Amicus Br. for Ireland 3-5.

Even if there were not an MLAT between the United States and Ireland, the government could have pursued its inquiry through a letter rogatory. "Letters rogatory are the customary method of obtaining assistance from abroad

---

23. U.S.-Ireland Mutual Legal Assistance Treaty, Art 1 § 1; § 2(b), (f).

in the absence of a treaty or executive agreement."[24] "A letter rogatory is a request from a judge in the United States to the judiciary of a foreign country requesting the performance of an act which, if done without the sanction of the foreign court, would constitute a violation of that country's sovereignty."[25] While it is true that actions requested in a letter rogatory can take a long time because they require the signature of a judge and, typically, transmittal through "diplomatic channels," it is also true that the time "may be shortened by transmitting a copy of the request through Interpol."[26]

The United States and the E.U. also have negotiated the U.S.-E.U. Data Privacy and Protection Agreement (DPPA), an "umbrella" agreement, which allows for the transfer of personal data between E.U. and U.S. law enforcement in criminal investigations, subject to certain privacy protections for personal data.[27] In connection with the DPPA, Congress passed the Judicial Redress Act of 2015, which provides the right for E.U. citizens to seek judicial redress in the United States if a privacy breach occurs. See Judicial Redress Act of 2015, Pub. L. No. 114-126, 130 Stat. 282.

---

24. U.S. Attorneys' Manual, Criminal Resource Manual § 276, "Letters Rogatory."

25. *Id.*

26. *Id.*

27. See Agreement Between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses, U.S.-E.U., Jun. 2, 2016, available at https://www.justice.gov/opcl/DPPA/download (last visited Jan. 15, 2018).

Moreover, the United States has previously participated in devising multinational solutions to cross-border evidentiary discovery and transfers of personal data for commercial use. For example, the Hague Convention on Taking of Evidence Abroad in Civil or Commercial Matters sets forth a number of procedures for obtaining documents and testimony from people and places abroad in instances where application of U.S. rules might unnecessarily complicate diplomatic relations.

The government therefore has existing multilateral options for obtaining data abroad. It also can establish new multilateral processes that address both domestic law enforcement needs and the delicate, foreign policy interests that are unavoidably implicated by the transnational nature of data collection and storage.

CONCLUSION

For the foregoing reasons, amici urge this Court to affirm the judgment of the court of appeals.

Respectfully submitted.

ILANA H. EISENSTEIN
Counsel of Record
ETHAN H. TOWNSEND
JOHN M. LEITNER
LINDSAY R. BARNES III
DLA PIPER LLP (US)
One Liberty Place
Philadelphia, PA 19109
(215) 656-3300
ilana.eisenstein@dlapiper.com

Counsel for Amici Curiae

APPENDIX

APPENDIX — DIGITALEUROPE'S MEMBERS

Amici DIGITALEUROPE's member companies include: Adobe, Airbus, Amazon, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Intel, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, and Zebra Technologies.

DIGITALEUROPE's member trade associations are:

Austria:	IOÖ
Belarus:	INFOPARK
Belgium:	AGORIA
Bulgaria:	BAIT
Cyprus:	CITEA
Denmark:	DI Digital, IT-BRANCHEN

Appendix

Estonia:	ITL
Finland:	TIF
France:	AFNUM, Force Numérique, TECH IN France
Germany:	BITKOM, ZVEI
Greece:	SEPE
Hungary:	IVSZ
Ireland:	TECHNOLOGY IRELAND
Italy:	Anitec-Assinform
Lithuania:	INFOBALT
Netherlands:	Nederland ICT, FIAR
Poland:	KIGEIT, PIIT, ZIPSEE
Portugal:	AGEFE
Romania:	ANIS, APDETIC
Slovakia:	ITAS
Slovenia:	GZS
Spain:	AMETIC

Appendix

Sweden:	Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland:	SWICO
Turkey:	Digital Turkey Platform, ECID
Ukraine:	IT UKRAINE
U.K.:	techUK